Technical Cybersecurity

Types of Campaigns

Types of Campaigns

Criminal

- Primary goal is $$$$$

Nation-state

- Information or sabotage

Organization

- Similar to Nation-State

Hobbyist

- General interest

Criminal Campaigns

Motivated by money

- But there's lots of ways to make money!

Large number of different models

- Botnets
- Ransomware
- Theft: credentials, carding, cash, extortion
- Tech support and other cons

Nation-State

Focused on national interest

- Similar to ideological

Different Goals

- Intelligence gathering
- Sabotage
- Information operations

Organizations

Terrorist, Corporate

- Wildly different motivations
- Terrorists are similar to Nation-State, corporate to Criminals

Terrorists

- Sabotage with high financial or human costs
- Need $$$ too
- Some intelligence gathering

Corporate

- IP protection

Hobbyist

Not much of this anymore

- Some, but interested in research

Criminal more easily differentiated

- Early hackers arrested, even when no mal-intent
- Now that we have real criminals, LE pays attention to that
- Things more serious, but less-hyped

Campaign Architecture

Each campaign has an architecture

- **Goals**: What do you want to accomplish?
- **Strategies**: How to you intend to achieve your goals?
- **Principles**: What are the rules of engagement? what are you willing to do, and what will you not do? is collateral damage acceptable or not? why?
- **Assets**: What assets do you have that you can use?
- **Tools**: What kind of tools to you have available, and will they work with your assets?
- **Tactics**: What kind strategies will you use? Phishing? Worms? Viruses? Trojans? physical entry and planting?

Theft & Extortion, Intelligence Operations, Sabotage

Let’s learn about theft and extortion!